DIGITAL CERTIFICATES

There has been some confusion regarding the process to apply for and download digital certificates and the importing/exporting process for your certificate once you have it.

WHO NEEDS DIGITAL CERTIFICATES? At this time any operator that accesses UCCH, Triple I or NLETS for criminal history purposes using the browser enabled access is required to have a digital certificate for identification purposes. Agencies using either the DPS provided, or other vendor supplied (such as PSI) or self-written program for socket access are not required to use digital certificates. For this article we are only going to concern ourselves with the digital certificate application process.

BROWSER: Agencies using the browser enabled access must use the Internet Explorer browser to access the system. The browser version must be a minimum of 5.5 with service pack 2, but agencies are encouraged to upgrade to version 6.0 if possible. (There are some connectivity issues that are corrected with version 6.0 if your operating system will function with that version.)

To ascertain which browser version you are using, open your browser and click on **Help** at the top of the screen. Select **About Internet Explorer** from the drop-down menu and it will display the version information.

There are three steps to obtain a digital certificate; Application, Authentication and Retrieval.

APPLICATION: Once you have verified your browser is compatible, go to www.digsigtrust.com/state/ut to begin the application process. Select **TrustID Personal Certificate**. A pop-up will display the instructions for this process. When you select **Next** it will advise you of the information you will need to complete your application. Press **Next** to continue. You will then be prompted to provide personal identification such as name and address. A couple of questions will ask if your home address or place of employment have changed within the last 6 months. If so, this does not preclude you obtaining a certificate, but you may be required to provide additional information to complete your application.

Answer the questions on the first page and click on **Next** to continue. The next screen asks you to provide date of birth, social security number and photo identification information. You will also need to provide an email address and home and work telephone numbers. (No personal information used in this application process can be used for any purpose other than the application process for digital certificates. The information provided cannot be sold or provided to any other party.)

The next phase requires you to create a passphrase. This is similar to a password but is a short phrase of 8-30 characters. It is case sensitive and the number of characters also includes spaces. You will also be prompted to select and provide answers for "secret questions" in case you forget your passphrase. These are simple questions and you must select three from the random list. The list changes from person to person as they enter the application process.

Once you have created your passphrase you will be prompted to review the information you have provided. To make changes you will need to select **Back.** To continue, assuming the information is complete, select **Next**. If you agree with the disclosure statement, select **Next** again. You will now be prompted to select your method of payment for the certificate. If you are using a credit card to purchase this certificate the billing information must match the information entered on the digital certificate. If your agency has purchased voucher numbers to apply for the certificate, select **Payment Voucher** and press **Next**. You will then be prompted to enter the voucher number you have been provided.

AUTHENTICATION: Once you have completed your application process you will receive notification

1

by email. Within a few days you will also receive an activation code by mail at the address you provided. Once you have your activation code you will need to open your browser and go to the web site provided in the letter to complete the digital certificate retrieval process.

RETRIEVAL: Once you have completed this process you will no longer need to go through the User Authentication process of signing onto the UCJIS system. To test the retrieval of the certificate each operator or TAC should export their certificate to a safe location such as a diskette or a LAN drive. If the digital certificate has not been exported to a safe location and a computer is replaced or a hard drive crashes, the certificate cannot be recovered, and a new certificate will have to be purchased.

EXPORT: To export the certificate, open your browser then click on **Tools** then **Internet Options** then select **Content** then click on the **Certificates** button. Select the certificate that you are going to export by clicking on it to highlight it, then click on the **Export** button. Follow the prompts for each screen as they come up:

1. Click **Next** on the welcome window
2. Select **Yes, export the private key** and click on **Next**
3. Select **Enable strong protection** under **Personal Information Exchange** if it is not already selected
4. Create a password. You will need to remember this password to use this certificate - save it in a safe place or create one you will always know.
5. At the prompt to specify a file, click on **Browse**, then select the drive you want to export your certificate to (typically the A: drive or a LAN directory)
6. Type your name (or whatever name you want) in the field provided and click on **Save** or press enter then click **Next**
7. Complete your export by clicking **Finish** at the **Completing the Certificate Export Wizard** frame. You will get a pop-up frame stating that you were successful
8. Type your name (or whatever name you want) in the field provided and click on **Save** or press enter then click **Next**

To import your certificate, open your browser then click on **Tools** then **Internet Options** then select **Content** then click on the **Certificates** button. Click on the **Import** button. Follow the prompts for each screen as they come up:

1. Click **Next** on the welcome window
2. At the prompt to specify a file, click on **Browse**, then select the drive from which you want to import your certificate (typically the A: drive or a LAN directory) and select the certificate you want to import and click **Open** or press enter, then click on **Next**
3. Type the password associated with that certificate (created at the time it was exported)
4. Do NOT check the box to **Enable strong key protection**. Doing so will require you to enter the password associated with this certificate every time it is used
5. Check the box to mark the private key as exportable if desired then click on **Next**
6. Accept the defaults of the **Certificate Store** by clicking on **Next** again, then click on **Finish** to complete the import
7. You will get a pop-up frame telling you that you were successful

BYPASSING: Any operator can have access to the UCJIS files if their logon is bypassed during the certificate application process. In this instance the bypass is a temporary step to allow access until the certificate is downloaded. Certificates can also be bypassed to allow access if an operator loses his certificate or in the instance of access problems regarding the digital certificate. Please note that bypassing a certificate does not solve all access problems. If an operator had a certificate and the access problem lies somewhere else, bypassing the certificates will not allow access. Additional troubleshooting will be required.

ORDERING DISSEMINATION LOGS
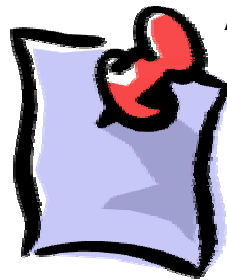
AGENCIES: Did you know that you can order dissemination logs from BCI anytime you need them?

To request a dissemination log for your agency, fill out the "Dissemination Log" form found in the Forms Section of your *BCI Operations Manual*. Please be sure to fill out the form completely to avoid delays.

When completed, mail the form to Nicole Starks at BCI. (The form can also be faxed to Nicole at 801-965-4749)

FBI BACKGROUND CHECKS ON INDIVIDUALS

BCI receives many questions from agencies regarding FBI background checks on individuals. If an individual wants an FBI background check on himself, the individual must submit:

1. A complete set of fingerprints on FBI form FD-258. The *Reason Fingerprint* block must contain **"Personal Records Check"**
2. A money order or certified check in the amount of $18.00, payable to the *U.S. Treasury*
3. A letter stating that the check is needed for personal reasons (the individual must be sure to include his/her name and return address)

Submit the above 3 items to:

CJIS Division
Attention: SCU
1000 Custer Hollow Road
Clarksburg WV 26306
Tel: (304) 625-3878

The findings of the background check will be mailed directly to the applicant. If no FBI record is found the fingerprint card will be stamped indicating "no record found". If there is a record found a copy of the record will be attached to the fingerprint card submitted (no stamp will be on the back of the fingerprint card).

The applicant cards and fingerprinting services are available at the Utah Bureau of Criminal Identification (3888 W 5400 S, SLC) Monday thru Friday from 8:00 am to 5:00 pm at a cost of $10.00 per person. Individuals can also check with their local police departments, motor vehicle offices, or private industries for these services. **Do not contact the FBI for fingerprinting.**

TAC CONFERENCE 2003

BCI's annual TAC Conference will be held May 13th and 14th, 2003 at Southern Utah University in Cedar City. (Same place as the last two years!) Attendance on May 13th is mandatory, and attendance on the 14th is optional. The conference fee is $45.00 per person for May 13th, or $60.00 per person for both days. There is a $10.00 per person discount for registrations paid on or before April 11, 2002.

Further information and registration forms have been mailed.

NCIC ENTRIES

As we at BCI prepare to go through the next cycle of compliance audits we would like to take an opportunity to remind all agencies that enter records into NCIC of a some items of interest.

First, please make sure that the record is as complete as possible. Where applicable, check all available files including, but not limited to:

1. Driver License
2. Motor Vehicle
3. Utah Criminal History
4. Triple I (Interstate Identification Index)
5. Juvenile Criminal History
6. Statewide Warrants and Protective orders

To make a complete entry, operators should first run the individual to ascertain if the warrant has already been entered. These files should be checked whether entering a wanted person or making a missing person entry.

Next, each entry into NCIC requires a second-party check. This is a quality control check to be performed by an operator other than the original operator that made the entry. This second party should again check each of the above listed files to ensure that all available identifiers and searchable information has been entered and accurate.

Please note that while the BCI Quality Assurance section makes every effort to review NCIC entries, they cannot review each and every entry. Nor should operators rely on their quality review to protect their agency from the liability of an inaccurate or incomplete entry.

Agencies must also remember that if a vehicle or person is in custody for a charge or reason other than the NCIC entry and will be held for a period of time, it is required that the agency requesting a hit confirmation use the "routine" status to allow one hour for confirmation of the entry. Using the "routine" status rather than the "urgent" status will help to prevent 2nd and 3rd hit confirmation errors. Most notably, the "urgent" status is being misused when a person is already in custody on another charge or a vehicle has been abandoned and the investigating officer requests an "urgent" request.

Another area of misuse is the sending of "locate" transactions to advise an agency that a hit needs to be confirmed. Please use the correct NLETS YQ/YR transactions to perform the hit confirmation process.

Lastly, if your agency receives a hit and the entering agency has placed extradition limitations that you are outside of, you MUST NOT use the NLETS YQ/YR transactions to confirm the hit. If this happens, your agency should contact the entering agency using an NLETS AM (administrative message) transaction or contact the entering agency via telephone. Many times the entering agency will confirm the hit and extradite from your location. However, it is a violation of NCIC policy to use the 10-minute hit confirmation request if you are outside of the extradition area. The only time you would use the NLETS 10-minute hit confirmation request is if the entering agency has requested you to do so, but only after contacting them prior to this.

FTP INFORMATION & CLASSES

UPDATE ON THE FTP UPGRADE: Those agencies who attended the recent FTP trainings at BCI will need to note some changes in the time frame of the move to the secured FTP server. The change to the new server that was supposed to happen on January 6, 2003 was delayed. At this time, a definite date to make the switch to the new server has not been determined. Agencies will need to continue to use the current means of getting bookings, audit reports and NCIC Validations.

Keep watching for word from BCI on when this change will take place.

If your agency didn't get the training for using the secured servers, you will need to attend the training on January 23, 2003. If you need to sign up, contact Della Miller at 801 965-4454 or email dimiller@utah.gov

NCIC VALIDATIONS

On July 1 2002, NCIC went into the final phase of NCIC2000. This means that all NCIC entries that need to be validated will have to be touched (modified) if they are to remain on NCIC. All untouched files will be automatically purged by NCIC. If your agency does not have access to NCIC on-line, you will need to make sure that a policy is in place with the entering agency on how your NCIC entries are to be validated.

There have been some questions about the responsibilities of non-terminal agencies and NCIC Validations. Now that we are in the final phase of NCIC2000, each validation will be performed on-line. This is accomplished by using a modify transaction in which the Name of Validator (VLN) Field is filled out for each NCIC entry. This constitutes validation and the NCIC2000 System inserts a Date of Last Validation (VLD) in the record.

Records that have been validated within the last calendar month are not retrieved for validation during the next validation cycle.

For more information on NCIC Validations, please refer to the *NCIC Operating Manual*, Introduction Section, 3.4, pages 54-57.

If you have any questions, please contact Della Miller at dimiller@utah.gov, or call at (801) 965-4454

10- PRINT CARDS AND NON-LIVESCAN SUBMITTING AGENCIES

With BCI's ability to electronically transmit fingerprint records to the FBI, it is no longer necessary to submit two fingerprint cards (pre-printed OTN and FBI) to BCI. Effective immediately, please submit only one pre-printed OTN card per incident. Please make sure the cards are completely filled out and that the fingerprint quality is readable. If you are in need of pre-printed OTN cards, please call Bobbi at 801-965-4943.

PERSONNEL CHANGE

Over the next couple of months two BCI staff members will be swapping duties. MaryAnn Curtis will take over the IBR statistical reporting position, while Adrienne Sowards will move to an auditing and training position.

WITNESS STATEMENT

We couldn't resist! Here is an actual witness statement from a traffic accident that occurred in a Salt Lake county agency in October:

"My buddy Nick saw the good looking police officer next to us. At a stop light. We were a little in front of her so I reversed to get next to her to have Nick ask for her name and number. I didn't see the car behind me and hit it."

The officer was kind enough to take the accident report, but she did not give Nick her phone number.

TOP TEN UCJIS TRANSACTIONS

UCJIS Transaction Counts For Nov, 2002

Transaction ID	Count
DQ Utah Drivers License	349,236
QW SWW/PO	291,207
RQ Utah Motor Vehicle	248,949
QV Query Vehicle	204,696
QW Query Wanted - NCIC	168,282
ID Ident/Authorized Transaction List	110,339
MIP Multiple Inquiry Person	89,821
IQ UCCH Name List	57,501
MIV Multiple Inquiry Vehicle	50,316
ACL Access Control List	44,829

UCR/IBR

WHY IS THE FBI ALWAYS TELLING US WHAT TO DO? Practically every agency that submits UCR/IBR data has asked this question.

So, why does it seem that the FBI is always telling you what to do?

The Uniform Crime Reporting program was established as a means of gathering data from agencies nationwide in a format that would allow for cross-jurisdictional comparisons. The only way data could be favorably compared would be to have all agencies use the same definitions and guidelines when *reporting* their crime statistics. This way, users of the data would not trying to compare apples to oranges.

Remember, this only pertains to *reporting* your crimes in UCR. How you charge and prosecute offenders is up to you!

In the next couple of years Utah NIBRS data will be made more accessible to Utah law enforcement agencies for analytical purposes. The more that agencies adhere to FBI reporting standards, the better the quality of data analyses. If agencies do not follow state and federal standards when reporting, the data in these databases will be almost worthless. Please do your part to ensure the integrity of the data.

2003 Year-End Report – It is time (*already?*) to start preparing the 2003 Year End Crime Report.

Please make sure all of your agency's 2003 UCR/IBR crime data is submitted to BCI as soon as possible. And our thanks to those agencies who have already sent in their full 12 months of data!

MISSING PERSON INFORMATION

PARENTAL ABDUCTIONS

The Criminal Justice System's Response to Parental Abduction

The Office of Juvenile Justice and Delinquency Prevention   (http://ojjdp.ncjrs.org)   recently conducted a study of agencies nationwide to gauge their actions and policies regarding parental abductions. The full study can be seen at http://www.ncjrs.org/html/ojjdp/jjbul2001_12_4/contents.html.

One of the findings of the study was that many agencies are underusing their state missing children's clearinghouses. All 50 states, the District of Columbia, and Puerto Rico now have state missing children's clearinghouses. These clearinghouses educate the public on missing children's issues, coordinate agency services aimed at child recovery, and provide assistance to law enforcement agencies in recovering children.

However, many investigators surveyed in the OJJDP study seemed unaware of the existence of the clearinghouse in their state or, if they were aware, did not convey to the researchers that they accessed clearinghouse services.

Is your agency using Utah's Missing Person's Clearinghouse to your full advantage?

Criminal and Civil Laws Regarding Parental Abduction

The Missing Children's Act of 1982 (28 U.S.C. §§ 534(a)). This Act requires the Federal Bureau of Investigation (FBI) to enter descriptive information on missing children into the National Crime Information Center (NCIC) database, a computer database with information on missing persons that can be accessed by law enforcement agencies nationwide.

The National Child Search Assistance Act of 1990 (42 U.S.C. §§ 5780). This Act requires that State and local law enforcement agencies immediately enter information on missing children younger than 18 into the NCIC database and prohibits such agencies from maintaining any waiting period prior to taking a report of a missing child.

The Parental Kidnapping Prevention Act of 1980 (28 U.S.C. §§ 1738A). Providing for civil remedies, this Federal Act gives jurisdictional priority to the child's home State in parental abduction cases where conflicts arise between two States. It extends the Federal Fugitive Felon Act to cases in which a child has been taken out of a State where that act would constitute a felony, thus enabling the FBI to investigate. It also authorizes certain persons access to the Federal Parent Locator Service for purposes of identifying the whereabouts of a parentally abducted child.

The Uniform Child Custody Jurisdiction Act (UCCJA). An important civil remedy that exists to combat parental abduction, this jurisdictional statute governs when a court has jurisdiction over a parental abduction case and attempts to prevent the occurrence of simultaneous proceedings in two different States. It has been enacted with some variation in all 50 States, the District of Columbia, and the Virgin Islands.

The Uniform Child-Custody Jurisdiction and Enforcement Act (UCCJEA). The Uniform Child-Custody Jurisdiction and Enforcement Act, adopted unanimously by the National Conference of Commissioners on Uniform State Laws in 1997 and approved by the American Bar Association in 1998, amends UCCJA to bring it into conformity with the Parental Kidnapping Prevention Act. UCCJEA also clarifies jurisdictional provisions of UCCJA that courts have interpreted inconsistently across the country. As of January 2001, 22 States had enacted UCCJEA.

RACHAEL ALERT

The Utah Rachael Alert is part of the nationwide Amber Plan, a voluntary partnership between law-enforcement agencies and broadcasters. The plan utilizes the Emergency Alert System to air a description of the missing child and suspected abductor. It has proven to be an effective way to quickly inform the public about serious child abduction cases. The goal is to instantly alert the entire community to assist in the search for and safe return of abducted children.

In Utah, the plan has been expanded to include electronic roadway signs, CB radio and other means to alert the public.

Utah adopted the Amber Alert on April 2, 2002 and launched a statewide program to issue Rachael Alerts. The Rachael Alert is named after Rachael Marie Runyan, who was kidnapped and killed in Utah in 1982. The parents of Rachael Runyon, law enforcement officers and broadcasters hope Rachael Alerts will help prevent similar tragedies. The Salt Lake City PD issued the first Rachael Alert after the kidnapping of Elizabeth Smart on June 5, 2002.

To date there is only one law enforcement agency in Utah known to have drafted a department policy for the Rachael Alert. The Utah County Sheriff's Office contacted the Missing Person Clearinghouse on assisting them with drafting the policy. They then put together a policy that will be carried out if a child abduction should take place in Utah County that fits the criteria for a Rachael Alert.

If your agency has questions about drafting a department policy or training with the Utah Rachael Alert, please contact Gina McMahon at 801-965-4686.

The Rachael Alert

- Powerful law-enforcement tool and wonderful way broadcasters can contribute to their communities.
- Sends a strong message that law enforcement and broadcasters are providing a proactive way to help protect their community's children.
- Provides each agency with a rapid response to serious child abductions.
- Dramatically increases law enforcement's ability to locate witnesses and resolve cases.
- Engages the entire community to mobilize and assist with recovering the child and apprehending the abductor.
- Acts as a deterrent to this type of crime.
- Builds relations between law enforcement, broadcasters, and the community.
- Costs very little to implement.